

Příloha 1 |

RFC Požadavky AIS a aktualizace dat

A. GUI / UX

1. Umožnit přihlášení uživatele bez role k AIS – CAAIS poskytuje (prázdný) seznam rolí.

Popis problému: Některým AIS stačí pro základní použití pouze autentizace uživatele, nemusejí ho autorizovat. Příkladem může být Service Desk DIA. Ostatně CAAIS nemá provádět autorizaci – ani k tomu nemá prostředky, pouze autorizační údaje poskytovat.

Požadované řešení: CAAIS umožní přihlásit se do AIS i uživateli, pokud ten nemá přiřazené žádné přístupové či agendové role. Vzhledem k nutnosti kompatibility s JIP/KAAS bude konfigurace AIS obsahovat přepínač „Vyžadovat přístupovou roli“ nastavující odpovídající příznak konfigurace AIS. Při pozitivním příznaku bude CAAIS při přihlašování stejně jako dosud ověřovat, zda má uživatel alespoň jednu přístupovou roli k danému AIS.

Přepínač „Vyžadovat přístupovou roli“ bude v části Doplnující údaje / Konfigurace AIS s hintem (bílé „i“ v černém kruhu): „Pokud uživatel nemá přiřazenou žádnou přístupovou roli, nebude mu přihlášení dovoleno. K zajištění kompatibility s JIP/KAAS.“

Akceptace: GUI upraveno dle zadání; úspěšné ověření funkcionality přihlášení v obou stavech příznaku.

2. Importovat AIS, jejich role a přiřazení rolí subjektů.

Popis problému: Před migrací uživatelů z JIP/KAAS by měl CAAIS poskytovat i role, ke kterým lze při migraci uživatele spárovat, jelikož aktuálně neexistuje mechanismus, jak přiřazení rolí domigrovat.

Návrh řešení: Dodáme ve vhodném formátu (CSV)

- seznam AIS jako zkratka_subjektu, název_ais, zkratka_ais, poznámka_ais;
- seznam rolí jako zkratka_ais, zkratka_role, název_role;
- seznam přiřazení rolí k subjektům jako zkratka_subjektu, zkratka_role.

a případně další atributy, které mohou či musí být přiřazeny k daným objektům v datovém modelu, respektive vloženy do tabulek v databázově relačním modelu.

Požadované řešení: Po ověření importu na stage či edu prostředí, bude ten spuštěn na produkci.

Akceptace: AIS, jejich role a přiřazení rolí k subjektům je naimportováno dle dodaných datových sad.

3. Předávat telefonní čísla AIS.

Popis problému: Některé systémy evidují vedle e-mailu i další kontakty na uživatele jako telefonní číslo. Jelikož CAAIS tento údaj eviduje, může jej předat, aby jej systém mohl předvyplnit. Současně při každém přihlášení může systém ověřovat, zda se kontakty nezměnily a případně nabídnout uživateli aktualizaci.

Požadované řešení: V rámci scope contact předávat i telefonní čísla v kanonickém formátu ITU-E.164. Úprava se týká jen moderních protokolů OIDC a SAML 2.0, nikoli JIP/KAAS. Předává se první mobilní telefonní číslo na profilu; pokud takové není, tak první telefonní číslo.

Poznámka: Protokolem SAML i OIDC lze podle všeho předat pouze jedno telefonní číslo (preferované je mobilní). Více telefonních čísel lze předat pouze v proprietární extenzi. Typ telefonního čísla se předávat nebude; ani v CAAIS není evidence typu telefonního čísla příliš smysluplná a může od ní být v budoucnu upuštěno.

Související: CAAIS by měl interně evidovat čísla ve formátu ITU-E.164. Validace vkládaných telefonních čísel by se tomu měla přizpůsobit (přijímat zahraniční telefonní čísla s mezinárodní předvolbou, u českých ji případně doplnit) a v tomto duchu by měly být aktualizovány i záznamy v databázi a případně upravena migrace z JIP/KAAS.

Reference:

- https://ec.europa.eu/digital-building-blocks/sites/download/attachments/467109280/eIDAS%20SAML%20Attribute%20Profile%20v1.4.1_final.pdf?version=1&modificationDate=1729176514404&api=v2
- <https://www.zakonyprolidi.cz/cs/2007-117#f5771302>

Akceptace: Protokoly SAML a OIDC předávají telefonní číslo uživatele dle zadání. Do profilu uživatele lze vložit zahraniční telefonní číslo. U českých telefonních čísel se validuje formální správnost na 9 číslic (po mezinárodní předvolbě).

4. Předávat příznak statutárního zástupce při přihlášení.

Popis problému: Některé systémy (aktuálně CMS 2.5) potřebují ověřit, že přihlašovaný uživatel je statutárním zástupcem. Tuto informaci by jim měl CAAIS zprostředkovat bez toho, aniž by si usurpoval poskytování referenčních údajů.

Požadované řešení: Přidání proprietárního boolean atributu v OIDC scope profil a v SAML odpovídající příznaku statutárního zástupce v CAAIS.

Akceptace: Protokoly SAML a OIDC předávají boolean atribut odpovídající příznaku statutárního zástupce v CAAIS.

5. Synchronizovat subjekty z RPP.

Popis problému: Některé subjekty nejsou vedeny v ROS, nýbrž pouze v RPP, z něhož by měly být do CAAIS synchronizovány včetně statutárních zástupců, což nyní nefunguje.

Pro skupinu subjektů (317 k 2025-03-21), které nejsou vedeny v ROS (nemají IČO), nefunguje načítání statutárních zástupců z RPP, což je jediným zdrojem takového údaje. Zároveň tyto subjekty mají ve sloupcích „Zapisovat údaje do registru osob“ a „CAAIS primárním editorem“ hodnotu „Ano“, když to u nich nemůže platit, protože vůbec nejsou v ROS. Zároveň platí, že mají přiřazenu nějakou právní formu, jako by to byla právnická osoba, což neodpovídá skutečnosti.

Požadované řešení: CAAIS přebírá z RPP aktualizace o změnách statutárních zástupců subjektů nevedených v ROS. Chybějící statutární zástupci budou jednorázově doplněni skriptem. Subjekty mimo ROS budou mít novou právní formu „nedefinováno“ (případně „subjekt mimo ROS“) a nebudou mít zaškrtnuté příznaky „Zapisovat údaje do registru osob“ a „CAAIS primárním editorem“.

Návrh řešení:

- Číselník právních forem je rozšířen o novou hodnotu.
- Příznaky „Zapisovat údaje do registru osob“ a „CAAIS primárním editorem“ budou pro identifikovanou množinu subjektů vynulovány.
- Bude upraven proces synchronizace s RPP.
- Bude provedena jednorázová synchronizace s RPP pro identifikovanou množinu subjektů.

Akceptace: Namátkou bude ověřeno, že údaje pocházející z RPP jsou aktualizovány a že se při změnách aktualizují.

6. Umožnit přidělení role lokálního administrátora i statutárnímu zástupci.

Popis problému: Na menších OVM může být statutárním zástupcem a lokálním administrátorem jedna osoba. I takový uživatel by měl mít možnost si aktivovat svůj profil v CAAIS IdP zasláním datové zprávy – postup získání role lokálního administrátora by neměl diskriminovat, zda jsou statutární zástupce a lokální administrátor dvě různé osoby, nebo jedna stejná osoba. Aktuálně tento způsob selhává.

Požadované řešení: Pokud je zaslána datová zpráva k založení lokálního administrátora, která by při neexistenci profilu ten založila, přidá taková zpráva roli lokálního administrátora k existujícímu profilu, který případně aktivuje, a aktualizuje jeho kontaktní údaje (s propsáním do CAAIS IdP).

Akceptace: Lze přidělit roli lokálního administrátora existujícímu profilu statutárního zástupce datovou zprávou.

7. Upravit konfiguraci napojení na NIA IdP.

Akceptace: Lze se autentizovat přes NIA.

8. Skrýt „Nahlásit problém“ v patičce CAAIS.

Popis problému: Aktuálně existuje pouze jeden kanál podpory CAAIS a to přes Service Desk. Ostatní kanály by uživatelé neměli využívat.

Požadované řešení: Skrýt buňku mřížky (element s atributem _ngcontent-ng-c439221885) s odkazem „Nahlásit problém“ v patičce CAAIS. Samotná akce může zůstat funkční.

Akceptace: V zápatí CAAIS se nezobrazuje výzva a odkaz k nahlášení problému přes formulář.

9. Změnit adresy sociálních sítí v patičce CAAIS a CAAIS IdP.

Popis problému: V zápatí CAAIS a CAAIS IdP vedou odkazy sociálních sítí DIA na nepoužívané účty.

Požadované řešení: Odkazy vedou na stejné adresy jako v zápatí na hlavní stránce dia.gov.cz. Myšlena je tím jednorázová změna adres k okamžiku řešení tohoto RFC.

Akceptace: Odkazy sociálních sítí vedou na stejné adresy jako v zápatí na hlavní stránce dia.gov.cz.